ABSTRACT OF THE DISCLOSURE

A server/overlay network architecture and related method prevent (i.e., minimize the likelihood of) overloads from many network clients all trying to upload data files to a common destination server on the network at about the same time. Before a client transfers its (his or her) data file to the common network destination, a unique identifier (generally much smaller than the data itself) for the data of that client is generated. The unique identifier, such as a one-way hash function, is transmitted to an authenticator trusted by the common destination. The authenticator time-stamps (i.e., stores time and date) the unique identifier, digitally signs a message incorporating the unique identifier and the time-stamp and sends the message to the client who sent the unique identifier. The client then sends the data file with its time stamp to one of a plurality of upload proxy servers. The proxy server sends a message to the common destination telling it to pick up the data file when ready. The common destination server thus avoids being overloaded by many clients transferring their rather large data files to it at the same time. The common destination server can check the time-stamp and unique identifier to insure that the data has not been altered after the time-stamp.